FIG. 1

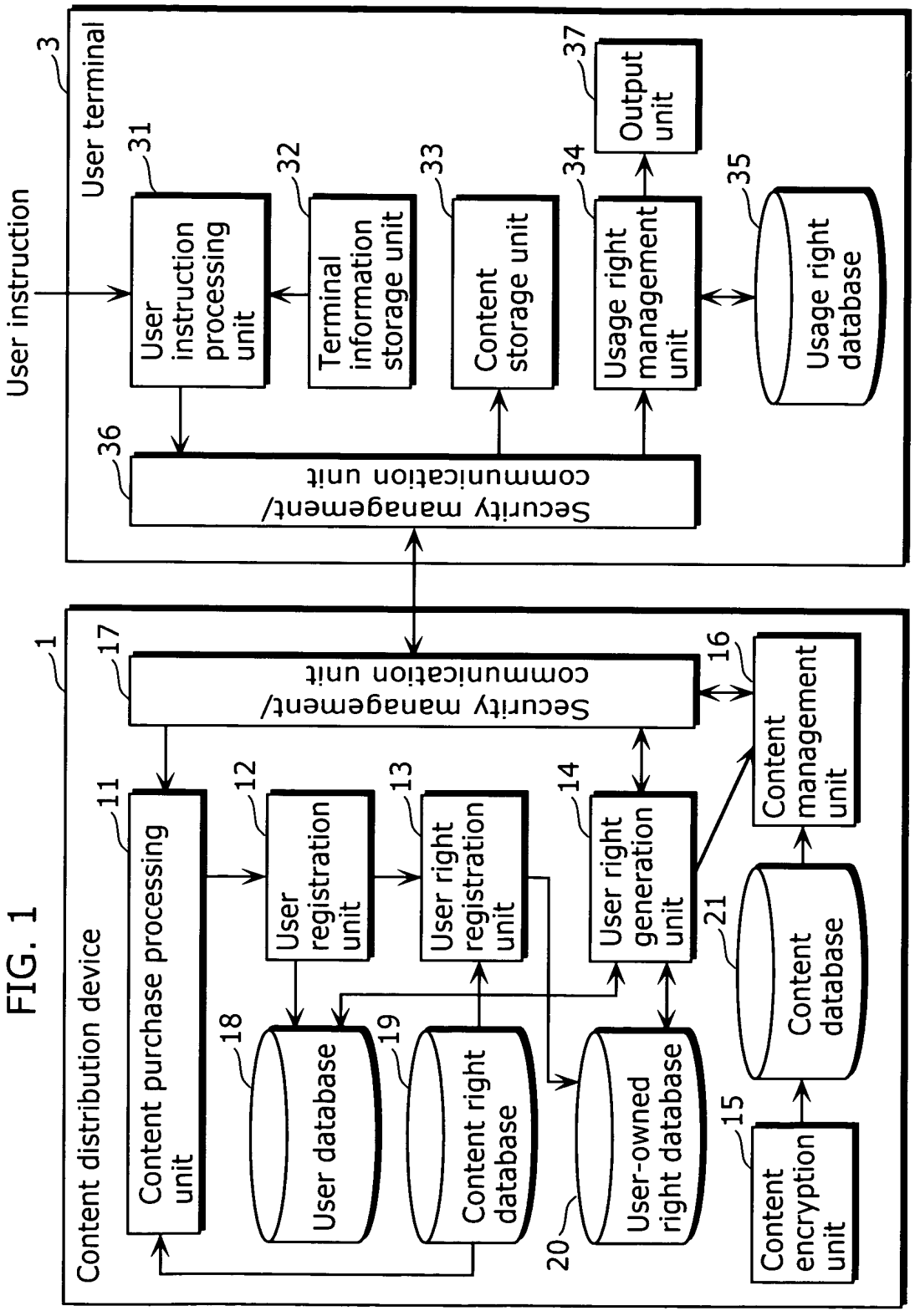

User terminal
3
User instruction
31
User instruction processing unit
32
Terminal information storage unit
33
Content storage unit
34
Usage right management unit
35
Usage right database
37
Output unit
36
Security management/ communication unit
Content distribution device
1
17
Security management/ communication unit
16
Content management unit
11
Content purchase processing unit
12
User registration unit
13
User right registration unit
14
User right generation unit
21
Content database
18
User database
19
Content right database
20
User-owned right database
15
Content encryption unit

FIG. 2

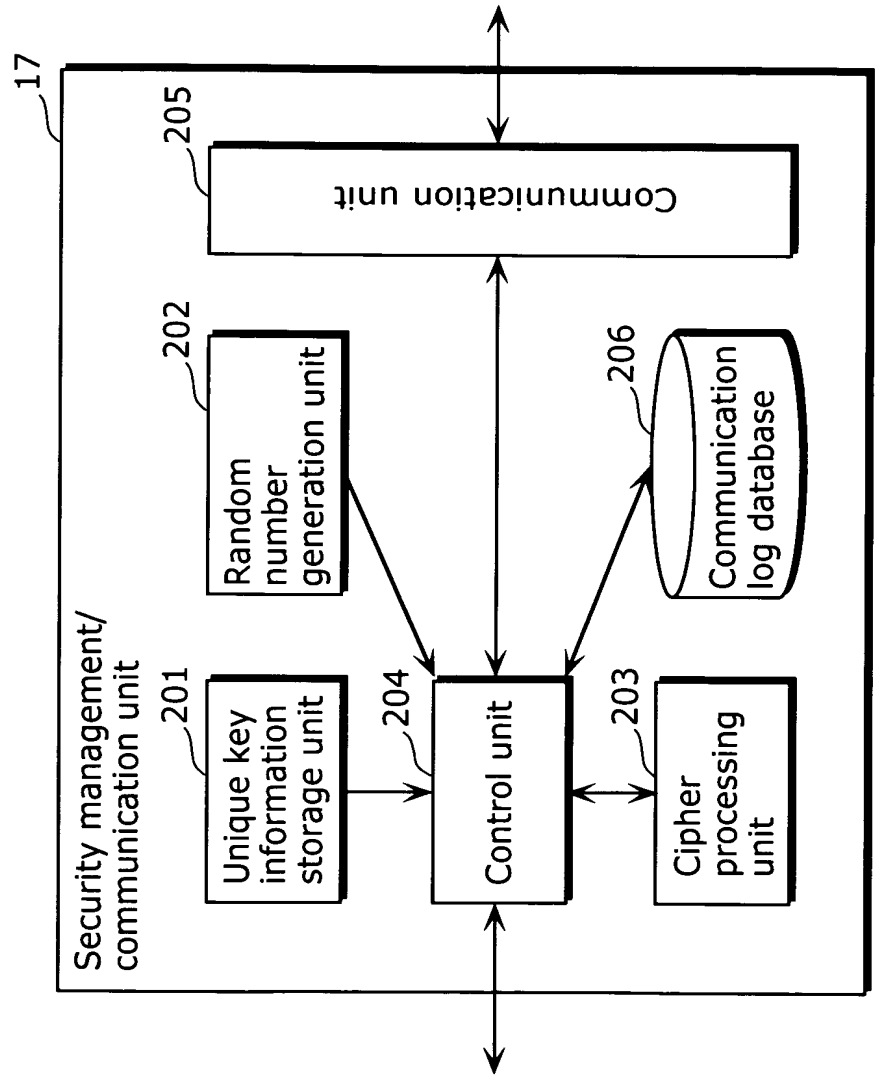

17
Security management/
communication unit
205
Communication unit
202
Random
number
generation unit
206
Communication
log database
201
Unique key
information
storage unit
204
Control unit
203
Cipher
processing
unit

FIG. 3

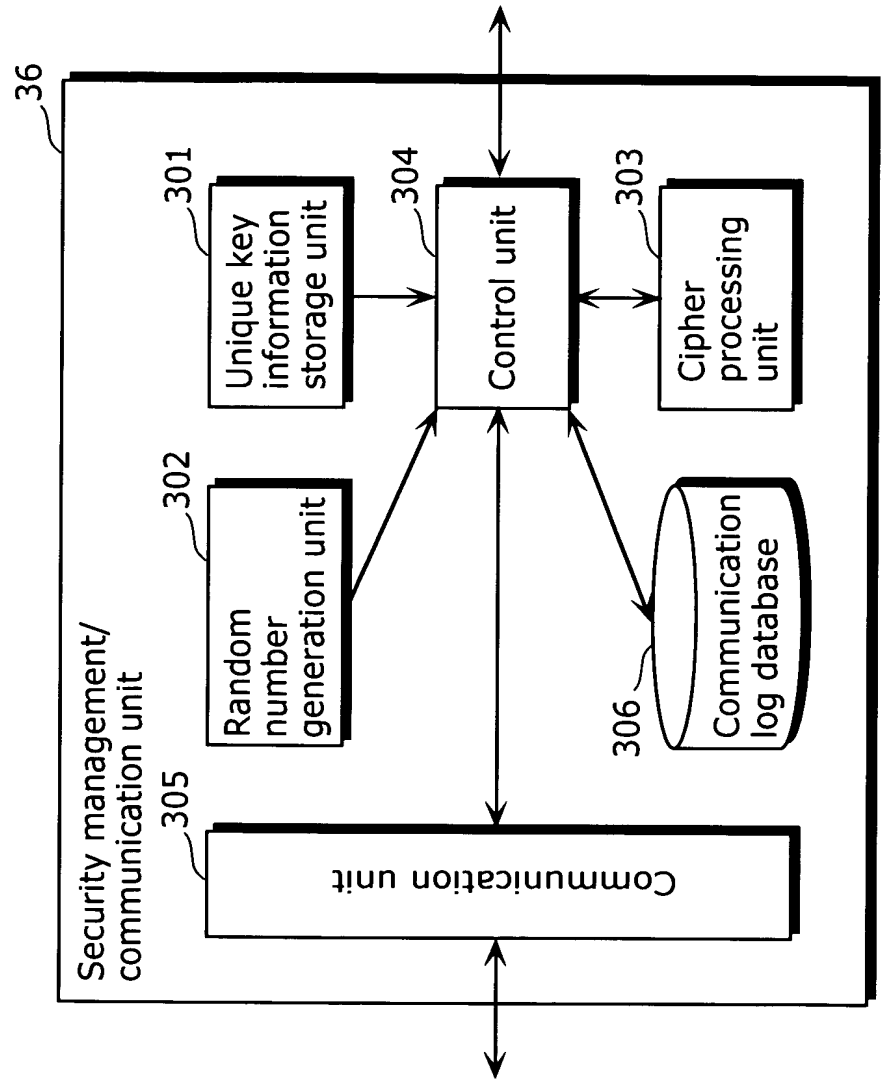

36
Security management/
communication unit
301
Unique key
information
storage unit
304
Control unit
303
Cipher
processing
unit
302
Random
number
generation unit
306
Communication
log database
305
Communication unit

FIG. 4

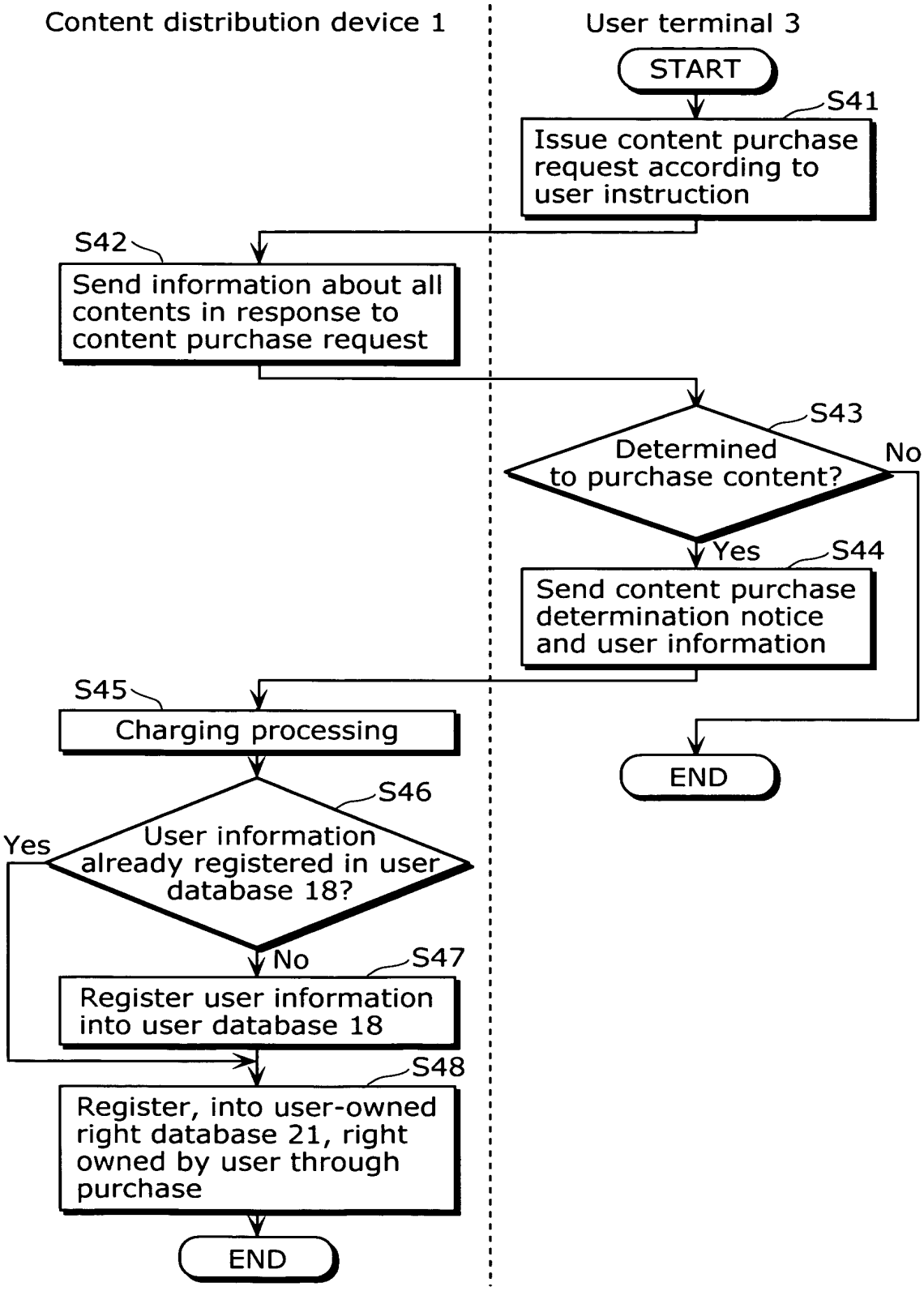

Content distribution device 1
User terminal 3
START
S41
Issue content purchase request according to user instruction
S42
Send information about all contents in response to content purchase request
S43
Determined to purchase content?
No
Yes
S44
Send content purchase determination notice and user information
END
S45
Charging processing
S46
User information already registered in user database 18?
Yes
No
S47
Register user information into user database 18
S48
Register, into user-owned right database 21, right owned by user through purchase
END

FIG. 5

Content name	Content ID	Usage condition	Fee
Movie A	112233	Number of reproductions=2	¥400
Music B	334567	Number of reproductions=5 Total reproduction time=1H	¥500 ¥1000
Game C	321098	Total reproduction time=2H Unlimited	¥700 ¥2000

FIG. 6

User ID	Content ID	Usage condition
0001	112233	Number of reproductions=2
0002	321098	Total reproduction time=2H

10/542683

FIG. 7

User ID	Content ID	Usage condition
0001	112233	Number of reproductions=2
0002	321098	Total reproduction time=2H

FIG. 8

Content ID	Content name	Content encryption key	File name
112233	Movie A	0123456789..	movieA.mpg
234567	Music B	7361278168..	musicB.wav

FIG. 9

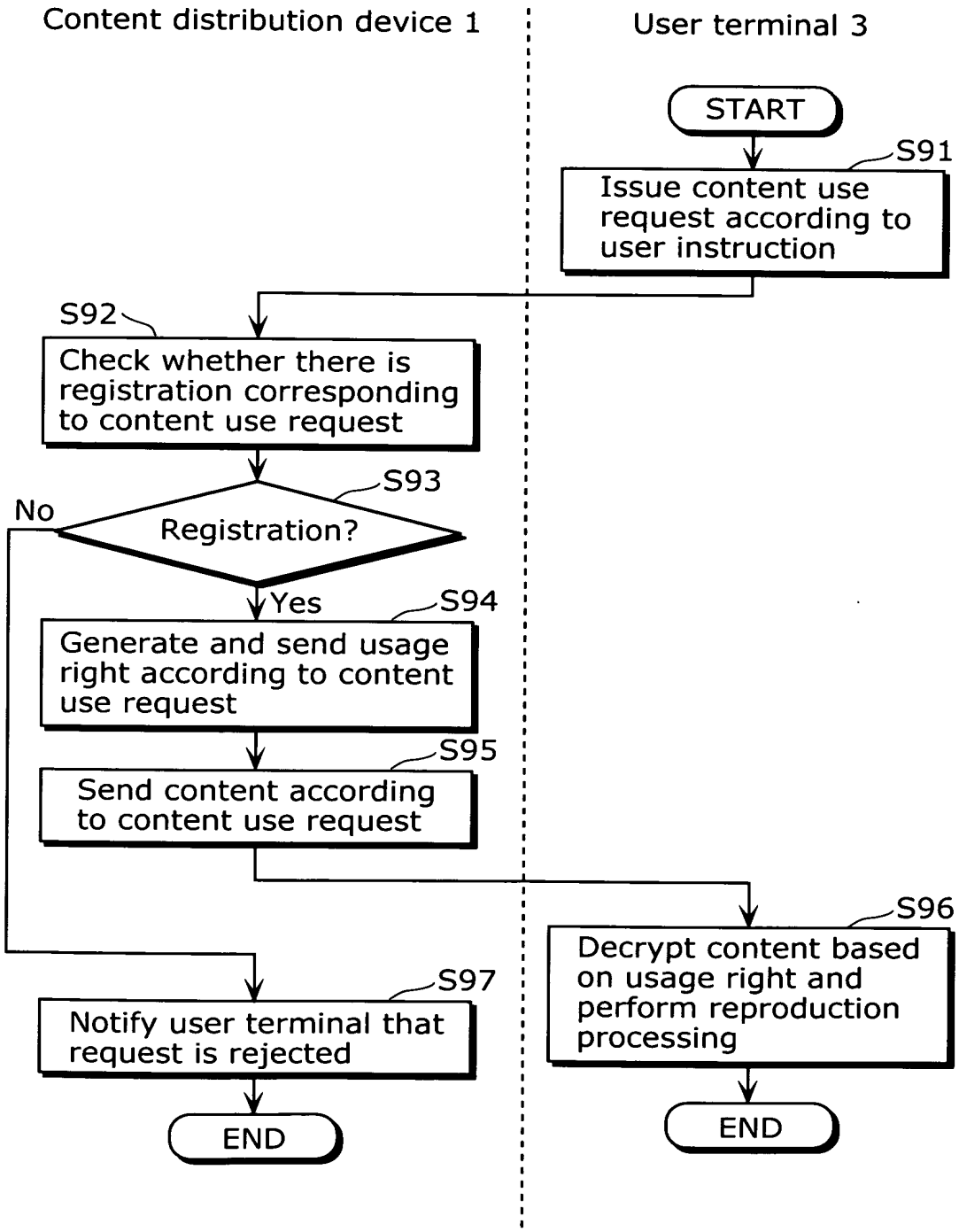

Content distribution device 1
User terminal 3
START
S91
Issue content use request according to user instruction
S92
Check whether there is registration corresponding to content use request
S93
Registration?
No
Yes
S94
Generate and send usage right according to content use request
S95
Send content according to content use request
S96
Decrypt content based on usage right and perform reproduction processing
S97
Notify user terminal that request is rejected
END
END

FIG. 10A

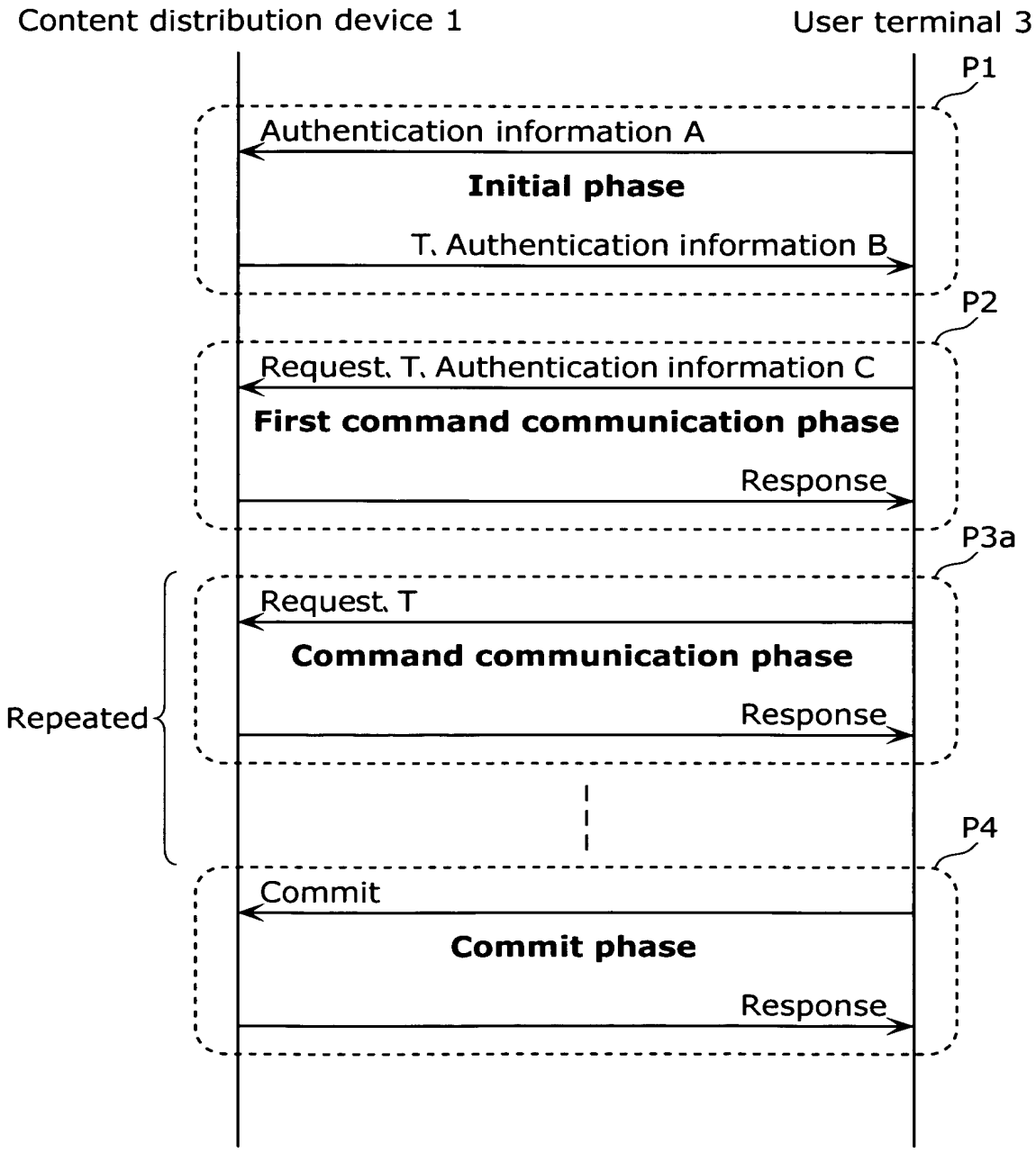

Content distribution device 1
User terminal 3
P1
Authentication information A
Initial phase
T, Authentication information B
P2
Request, T, Authentication information C
First command communication phase
Response
P3a
Request, T
Command communication phase
Response
Repeated
P4
Commit
Commit phase
Response

FIG. 10B

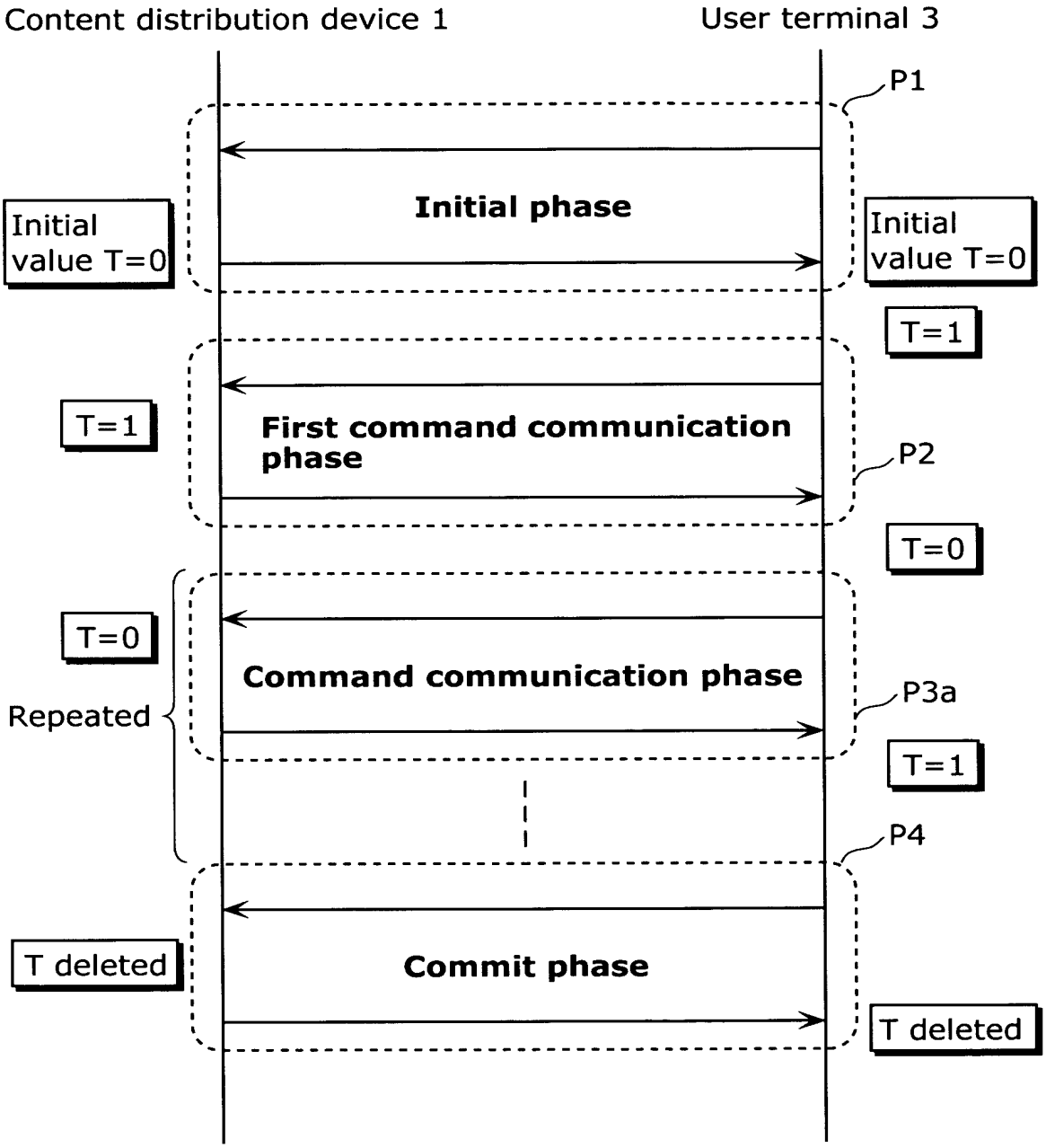

Content distribution device 1
User terminal 3
P1
Initial phase
Initial value T=0
Initial value T=0
T=1
T=1
First command communication phase
P2
T=0
T=0
Command communication phase
Repeated
P3a
T=1
P4
T deleted
Commit phase
T deleted

FIG. 10C

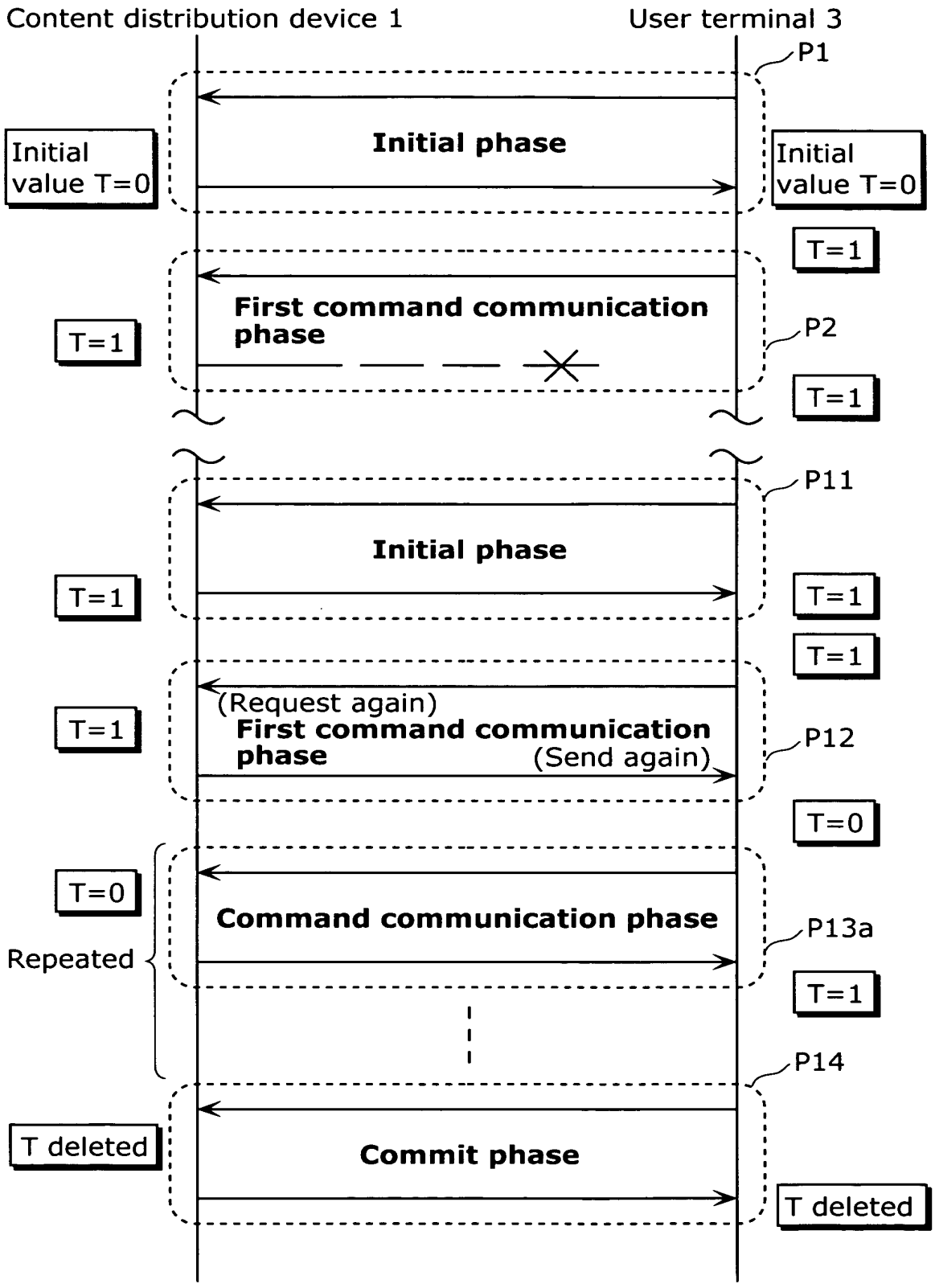

Content distribution device 1
User terminal 3
P1
Initial phase
Initial value T=0
Initial value T=0
T=1
First command communication phase
T=1
P2
T=1
P11
Initial phase
T=1
T=1
T=1
(Request again)
First command communication phase
(Send again)
T=1
P12
T=0
T=0
Command communication phase
Repeated
P13a
T=1
P14
T deleted
Commit phase
T deleted

FIG. 10D

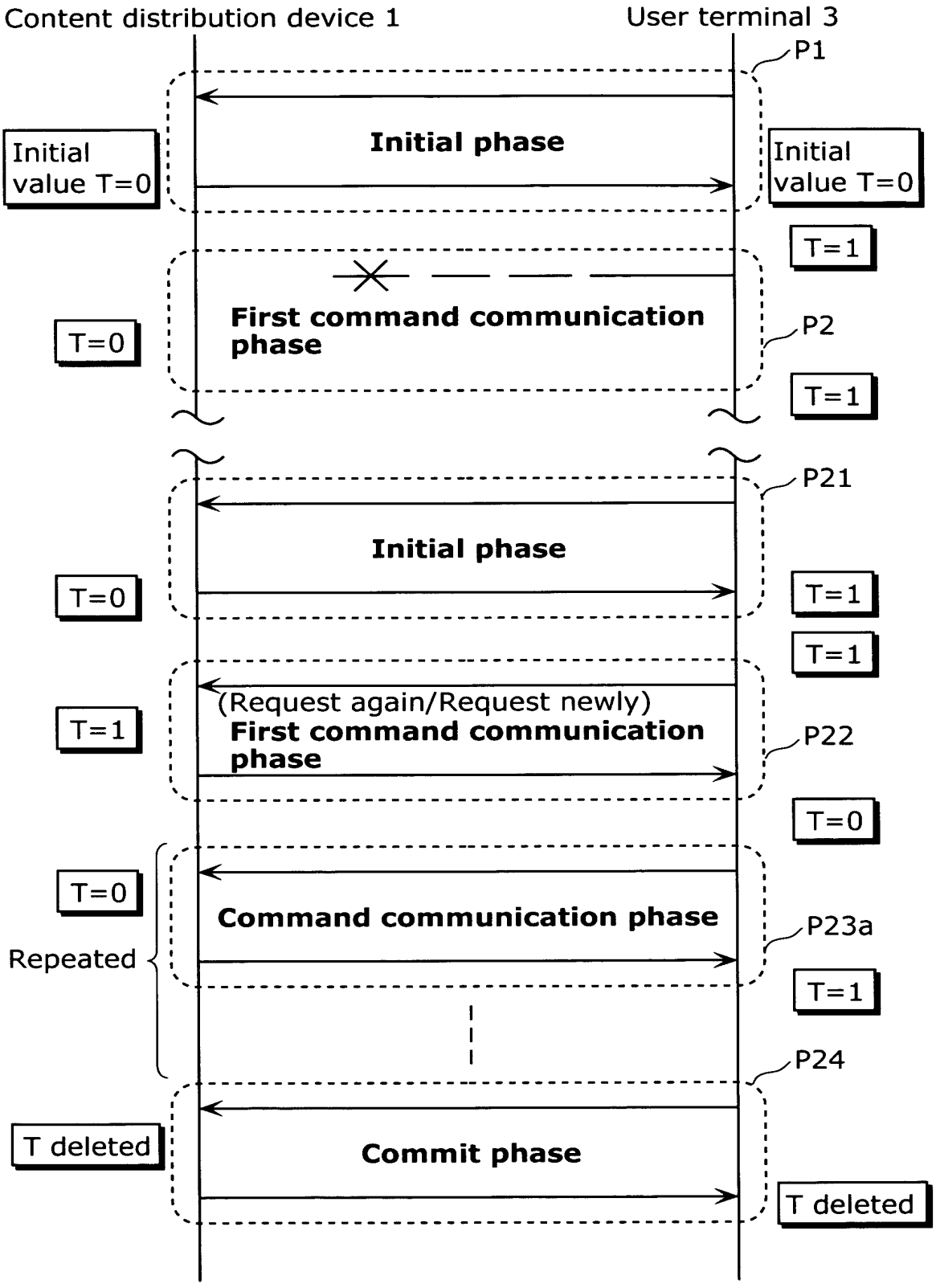

Content distribution device 1
User terminal 3
P1
Initial phase
Initial value T=0
Initial value T=0
T=1
First command communication phase
T=0
P2
T=1
P21
Initial phase
T=0
T=1
T=1
(Request again/Request newly)
First command communication phase
T=1
P22
T=0
T=0
Command communication phase
P23a
Repeated
T=1
P24
Commit phase
T deleted
T deleted

FIG. 11

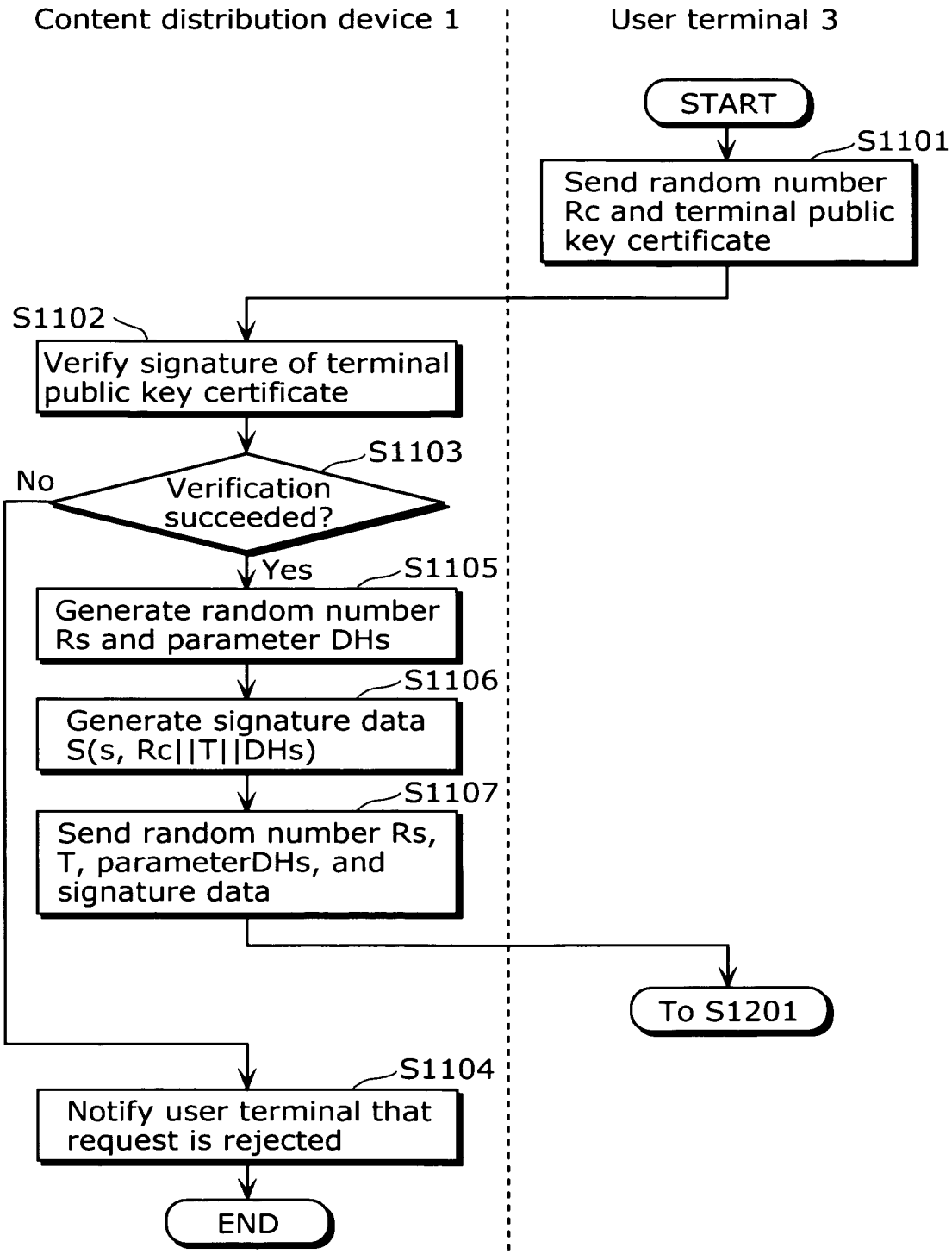

Content distribution device 1
User terminal 3
START
S1101
Send random number Rc and terminal public key certificate
S1102
Verify signature of terminal public key certificate
S1103
Verification succeeded?
No
Yes
S1105
Generate random number Rs and parameter DHs
S1106
Generate signature data S(s, Rc||T||DHs)
S1107
Send random number Rs, T, parameterDHs, and signature data
To S1201
S1104
Notify user terminal that request is rejected
END

FIG. 12

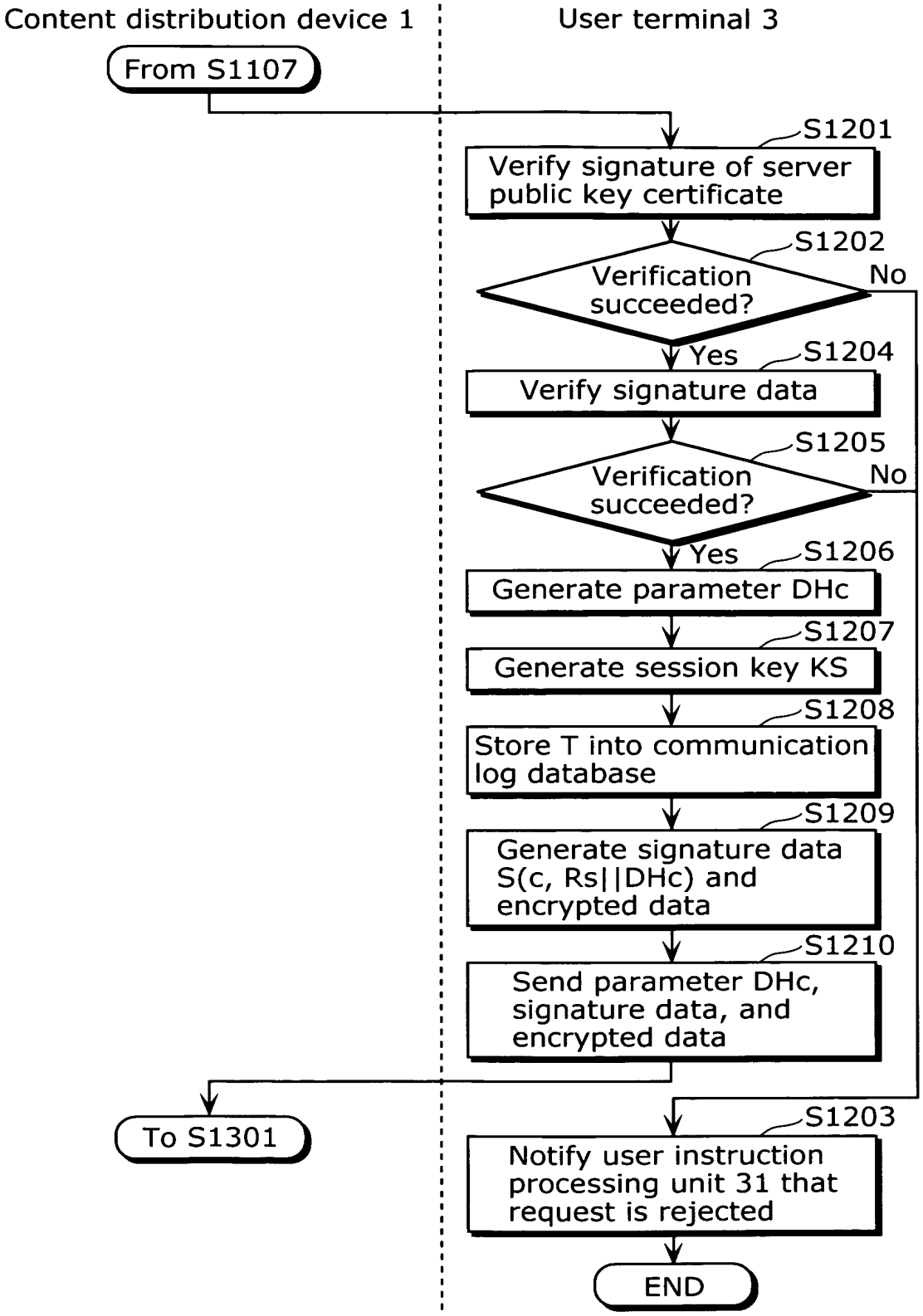

Content distribution device 1
User terminal 3
From S1107
S1201
Verify signature of server public key certificate
S1202
Verification succeeded?
No
Yes
S1204
Verify signature data
S1205
Verification succeeded?
No
Yes
S1206
Generate parameter DHc
S1207
Generate session key KS
S1208
Store T into communication log database
S1209
Generate signature data S(c, Rs||DHc) and encrypted data
S1210
Send parameter DHc, signature data, and encrypted data
To S1301
S1203
Notify user instruction processing unit 31 that request is rejected
END

FIG. 13

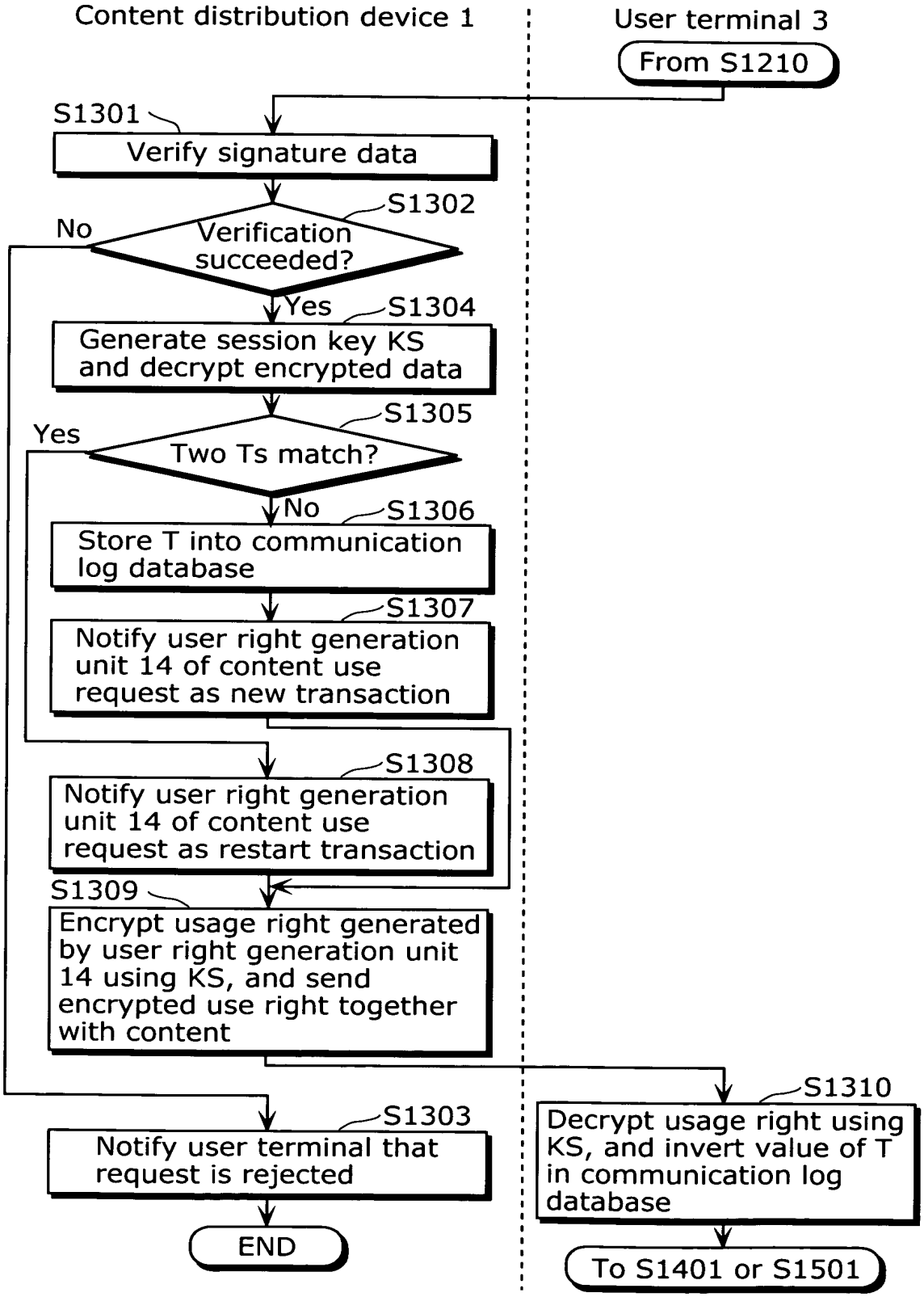

Content distribution device 1
User terminal 3
From S1210
S1301
Verify signature data
S1302
Verification succeeded?
No
Yes
S1304
Generate session key KS and decrypt encrypted data
S1305
Two Ts match?
Yes
No
S1306
Store T into communication log database
S1307
Notify user right generation unit 14 of content use request as new transaction
S1308
Notify user right generation unit 14 of content use request as restart transaction
S1309
Encrypt usage right generated by user right generation unit 14 using KS, and send encrypted use right together with content
S1310
Decrypt usage right using KS, and invert value of T in communication log database
To S1401 or S1501
S1303
Notify user terminal that request is rejected
END

FIG. 14

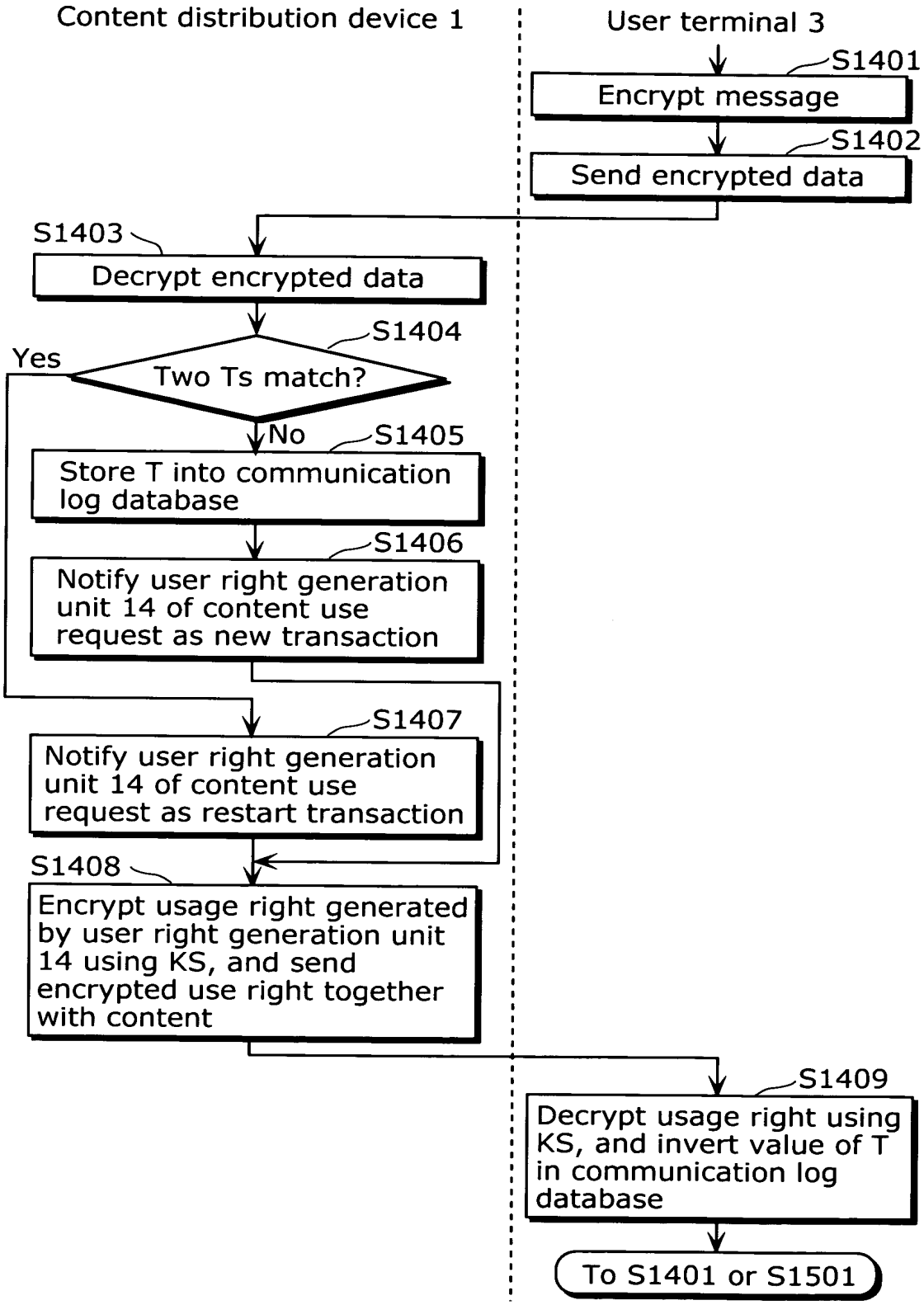
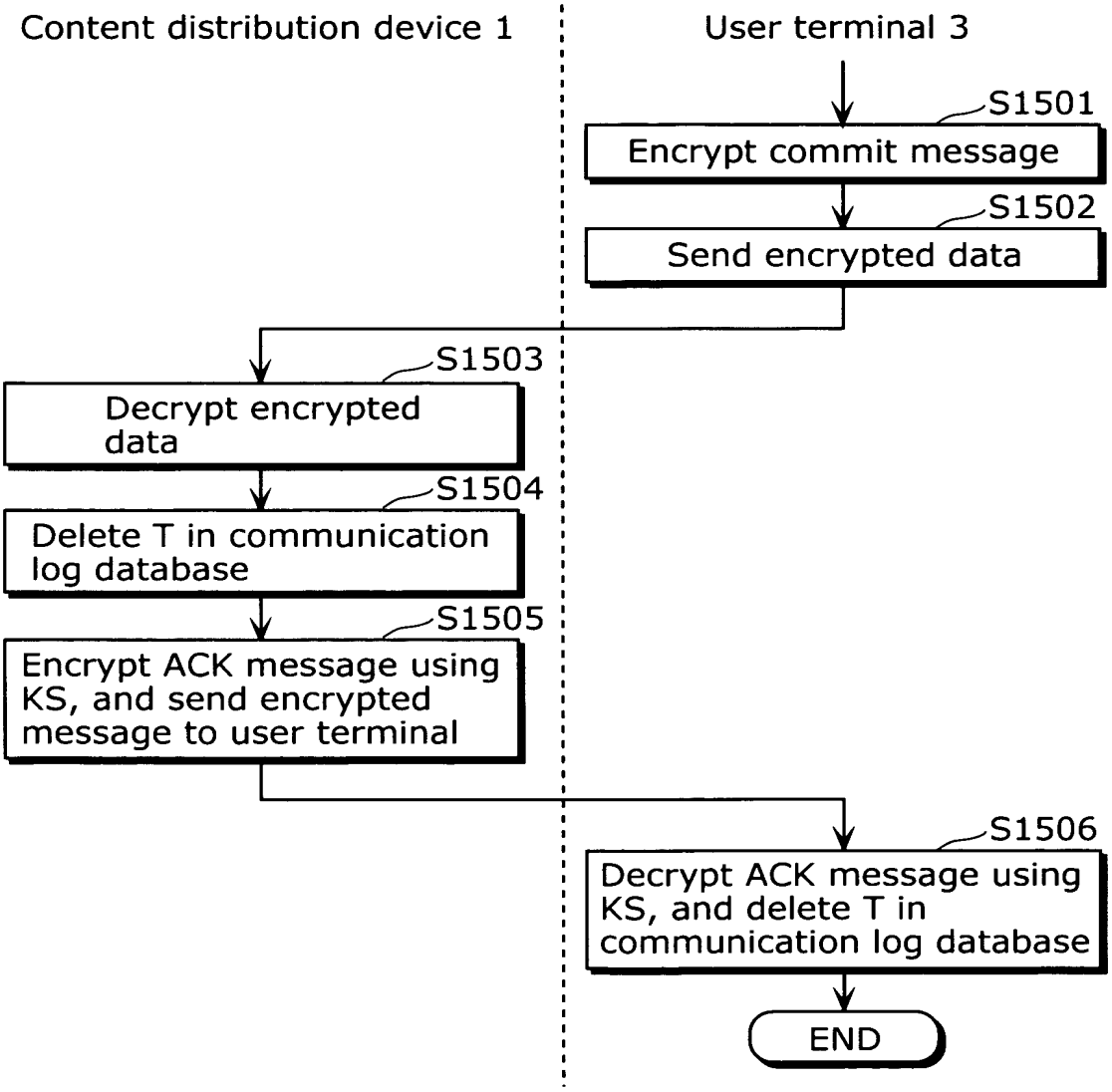

Content distribution device 1
User terminal 3
S1401
Encrypt message
S1402
Send encrypted data
S1403
Decrypt encrypted data
S1404
Two Ts match?
Yes
No
S1405
Store T into communication log database
S1406
Notify user right generation unit 14 of content use request as new transaction
S1407
Notify user right generation unit 14 of content use request as restart transaction
S1408
Encrypt usage right generated by user right generation unit 14 using KS, and send encrypted use right together with content
S1409
Decrypt usage right using KS, and invert value of T in communication log database
To S1401 or S1501

FIG. 15


Content distribution device 1
User terminal 3
S1501
Encrypt commit message
S1502
Send encrypted data
S1503
Decrypt encrypted data
S1504
Delete T in communication log database
S1505
Encrypt ACK message using KS, and send encrypted message to user terminal
S1506
Decrypt ACK message using KS, and delete T in communication log database
END